UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/620,364	07/17/2003	Colin John Blamires	03.028.01	8923

7590 03/05/2008

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
03/05/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 10/620,364
Filing Date: July 17, 2003
Appellant(s): BLAMIRES ET AL.

Kevin J. Zilka
Reg. No. 41,429
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 12/13/2007 appealing from the Office action mailed 5/15/2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

No amendment after final has been filed.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is not correct. Issue #4 is not present for review. There is no implied rejection under 35 U.S.C. §112.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,347,375	REINERT et al.	2-2002
6,721,883	KHATRI et al.	4-2004

Stallings, William. Network Security Essentials, Applications and Standards, November 1999 Prentice-Hall, Inc., pp. 320-323.

Yadav, Satyendra. "U.S. Patent Application Publication 2003/0149887 A1", August 2003.

McCoskey, John S. et al. "U.S. Patent Application Publication 2003/0028889 A1", February 2003.

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

1. Claims 1-3, 7-11, 15-19, 23-25 & 28-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent 6,347,375 to Reinert et al. (**Reinert**) in view of U.S. Patent Application Publication 2003/0149887 to **Yadav** and Network Security Essentials, Applications and Standards by **Stallings**.

Regarding claim 1, Reinert discloses a removable physical media (CD-ROM, col. 6, line 66) bearing a computer program (bootable virus utility, col. 6, lines 55-56) operable to control a computer to detect malware (viruses) by

performing the steps of booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media(CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28), and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations "establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer". However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database

with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been

motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 2, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 3, Reinert discloses wherein said steps further comprise loading security management code (communications program, col. 7, lines 65-67) operable to control said downloading (col. 8, lines 20-25).

Regarding claim 7, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 8, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 9, Reinert discloses booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote

computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25), performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28) and establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations "establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer". However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote

computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 10, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus

signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 11, Reinert discloses wherein said steps further comprise loading security management code (communications program, col. 7, lines 65-67) operable to control downloading (col. 8, lines 20-25).

Regarding claim 15, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 16, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 17, Reinert discloses a computer (computer 42, col. 7, line 60), said computer comprising a processor (CPU, col.6, lines 39-40) performing the steps of booting said computer with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from said removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, loading network support code (communications program) for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), downloading from a remote computer (remote computer 54) one or more malware (virus) detection files (col. 8, lines 20-25) , performing malware (virus) detection upon said computer using said one or more malware (virus) detection files (col. 8, line 28) and establishing a network

connection to said remote computer (col. 7, lines 4-5 & lines 65-67), wherein the network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to said remote computer (col. 7, lines 4-5 & lines 65-67). Reinert lacks the limitations "establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer". However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a

controlled link and to erect an outer security wall or perimeter (p. 320) and describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 18, Reinert discloses wherein said one or more malware detection files include at least one of malware definition data (up-to-date virus signature) containing data characteristic of malware to be detected (col. 8, lines 23-25).

Regarding claim 19, Reinert discloses wherein said steps further comprise loading security management code (communications program, col. 7, lines 65-67) operable to control said downloading (col. 8, lines 20-25).

Regarding claim 23, Reinert discloses an optical disk (CD-ROM, col. 6, line 66).

Regarding claim 24, Reinert discloses the malware to be detected including a computer virus and data file associated with a malware file (signature, col. 6, lines 55-56 & col. 8, lines 20-25).

Regarding claim 25, Reinert discloses a server computer (remote computer 54, col. 8, lines 10-11) connected by a network link to a computer (computer 42, Fig. 2), said server computer comprising a processor (inherent) configured to perform the steps of establishing a network connection to said remote computer (col. 7, lines 4-5 & lines 65-67), loading one or more malware (virus) detection files (col. 8, lines 20-25) to said computer, wherein said computer is booted with a non-installed operating system (bootable virus utility, col. 6, lines 55-61) read from a removable physical media (CD-ROM, col. 6, line 66) instead of an installed operating system (col. 6, lines 55-61) stored on said computer, wherein network support code (communications program) is loaded for said computer read from said removable media (CD-ROM, col. 7, lines 65-67), wherein said network support code (communications program, col. 7, lines 4-5 & lines 65-67) is used to enable said computer to establish a connection to

said server computer (col. 7, lines 4-5 & lines 65-67), wherein malware detection is performed upon said computer using said one or more malware detection files (virus definition files, col. 8, line 10-11 & line 28). Reinert lacks the limitations "establishing a secure network connection to said remote computer, wherein a firewall computer disposed between said computer and said remote computer is operable to block a connection between said computer and said remote computer of than said secure network connection, wherein said network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer". However, Yadav teaches that a computer (NDIS) scanning for potential intrusions uses a signature database for comparison with files (¶42) and updates the database with the latest intrusion signatures by contacting a remote computer (SOC, ¶42) over a VPN or SSL connection to safeguard the updates (¶¶43-44). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to connect to the remote computer via a secure connection and to enable the network support code to establish said secure connection to said remote computer. One of ordinary skill in the art would have been motivated to perform such a modification to safeguard the updates, as taught by Yadav (¶¶42-44). Further, Stallings describes that firewalls are inserted between the premises network and the Internet to establish a controlled link and to erect an outer security wall or perimeter (p. 320) and

describes the general characteristics of a packet-filtering firewall (p. 322), one being that a firewall forwards or discards packets (blocks connections, p. 322, §Packet-Filtering Router). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert, as modified previously by Yadav, to explicitly include, in a system comprising the removable physical media, a firewall between the computer (connected to the Internet) and the remote computer (private network, see also p. 323, Fig. 10.1(a)) that is operable to block a connection (discard packets) between said computer and said remote computer other than said secure network connection and for the support code to establish the secure network connection via the firewall. One of ordinary skill in the art would have been motivated to perform such a modification to establish a controlled link and to erect an outer security wall or perimeter between the computer and remote computer, as taught by Stallings (pp. 320-323).

Regarding claim 28, Reinert discloses wherein said remote computer (remote computer 54) determines said one or more malware detection files that are downloaded to said computer (downloaded under the control of remote computer 54, col. 8, lines 10-25).

Regarding claim 29, Reinert discloses wherein said one or more malware detection files are determined based on said non-installed operating system

(the malware detection files and service program must be able to run on the booted operating system, col. 8, lines 14-16 & lines 25-31).

Regarding claim 30, Reinert discloses wherein said one or more malware detection files (virus detection signature file) are determined based on a malware detection product (the virus detection signature file is used by the virus scanning software utility program, col. 8, lines 20-35).

2. Claims 26-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Reinert**, **Yadav** and **Stallings**, as applied to claim 1 above, in further view of U.S. Patent 6,721,883 to Khatri et al. (**Khatri**).

Regarding claim 26, Reinert lacks wherein said computer is configured in its BIOS settings. However, Khatri teaches that computer systems boot from a specific device (col. 1, lines 16-17) by scanning through a boot order (col. 1, lines 35-39) that is determined by a BIOS setup routine (col. 4, lines 15-17). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert to configure the BIOS settings to boot from said removable physical media. One of ordinary skill in the art would have been motivated to perform such a modification to allow a modern computer system to boot from the CD-ROM of Reinert, as taught by Khatri (col. 1, lines 16-17, lines 35-39 & col. 4, lines 15-17).

Regarding claim 27, Reinert lacks wherein booting said computer with said non-installed operating system read from said removable physical media is based on a determination that a bootable removable media is present. However, Khatri teaches that computer systems boot from a specific device (col. 1, lines 16-17) by scanning through a boot order (col. 1, lines 35-39) such that the system attempts each device in a specific order (i.e. determines if each device can be boot from and boots from the first available, col. 1, lines 35-39). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Khatri to base the booting the computer with said non-installed operating system on a determination that the removable media is present. One of ordinary skill in the art would have been motivated to perform such a modification to use a standard computer boot order to boot from Reinert's CD-ROM, as taught by Khatri (col. 1, lines 16-17, lines 35-39 & col. 4, lines 15-17).

3. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Reinert**, **Yadav** and **Stallings**, as applied to claim 1 above, in further view of U.S. Patent U.S. Patent 2003/0028889 to McCoskey et al. (**McCoskey**).

Regarding claim 31, Reinert lacks wherein said remote computer logs said downloading of said one or more malware detection files by said computer. However, McCoskey teaches a content delivery system such that when content

is downloaded to a client, a delivery server logs the download so that billing servers can determine if the user will be charged a fee (¶126). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify Reinert's remote computer such that it logs the downloading of one or more malware detection files. One of ordinary skill in the art would have been motivated to perform such a modification to allow a billing server to charge a fee for the download, as taught by McCloskey (¶126).

(10) Response to Argument

Issue #1:

Group #1: Claims 1-3, 7-11, 15-19, 23-25 & 28

Appellant's brief (pp. 11-12) argues that because Reinert teaches an invention used for providing up-to-date virus scanning comprising situations where the normal operating system of the local computer is not operable and that Yadav teaches a system where the computers contacting a remote server are operating normally, the prior art references could not be combined. It is first noted that col. 7, lines 49-51 uses the language "even if" to describe the event where the local operating system is not operable and as such it is not a requirement of Reinert that the local operating system be nonfunctional. The invention disclosed also works in those situations where the local operating system is not operational. Further, as stated in the rejection, Yadav is cited for teaching a benefit of creating a secure connection (as opposed to a non-

secure connection), such as a VPN or SSL connection, when updating signatures/definitions for an intrusion detection system. As Reinert's invention comprises a working virus scanning program that contacts a remote server (described at least at Reinert, col. 7, lines 49-67), Reinert's invention would equally benefit from the increase security and integrity of a secure connection between the local computer and the remote server.

Appellant's brief (pp. 12-13) argues the following:

> "disclosing that a user may connect to a remote computer utilizing a communications program (see Reinert), utilizing a VPN or a SSL to create a secure connection (see Yadav), along with a general firewall description (see Stallings), fails to specifically teach that "network support code is used to enable said computer to establish said secure network connection via said firewall computer to said remote computer".

However, Reinert discloses a system that utilizes a bootable media to boot a computer and execute a virus scanning application and to further execute a communications program (the claimed support code) to contact a remote server for, among other things, downloading updates to virus definition files (see col. 7, lines 49-67and specifically, col. 7, line 65 – col. 8, line 1 & col. 8, lines 23-25). A firewall is an application/device that protects a local system or network from network-based security threats (Stallings, p. 320, ¶1) where only authorized traffic will be allowed to pass (Stallings, p. 321, first #2 bullet point). Therefore, it is obvious to modify Reinert, as modified by Yadav, to include a firewall to protect the remote server from network-based security threats by installing a firewall to

allow only authorized connections (i.e. the connections from the local computer), as taught by Stallings. The firewall examines packets and passes or discards the packets based on rules (Stallings, p. 322). As described above, Reinert (and Reinert, as modified by Yadav) teaches a program (the claimed support code) establishing a network communication from the local computer to a remote server. Therefore, Reinert discloses "wherein said network support code is used to enable said computer to establish said secure network connection". The question raised is whether the support code (Reinert's communication program) would enable said computer to establish the connection via the firewall. However, it is submitted that because network traffic is already produced by Reinert's communications program (the claimed support code), Reinert's communication program has the functionality to "enable a connection to the remote computer via the firewall". This is because the firewall alone decides what traffic is passed, not the communications program, and as described above, it is obvious for the firewall protecting the remote server to allow the traffic from Reinert's local computers to the remote server, as this is the traffic that is required to be authorized for Reinert's invention to work.

Group #2: Claim 29

Appellant's brief (p. 14) argues that "simply disclosing that a program is downloaded from the remote computer to the local computer and may be

executed in local memory, as in Reinert, fails to even suggest that "one or more malware detection files are determined based on said non-installed operating system" (emphasis added)". However, the broad limitation "based on" is not defined as such to require any specific connection or procedure tying the non-installed operation system with the malware detection files. It is submitted that since Reinert's non-installed operating system (Reinert's virus scanning program with communications program, Reinert col. 7, lines 62-67) retrieves the malware detection files (up-to-date virus signature file, col. 8, lines 20-25), the downloaded malware detection files are determined based on the virus scanning program and the communications program (non-installed operating system). In the realm of Reinert's invention, the malware detection files would not be downloaded without the non-installed operating system and thus are determined "based on the non-installed operating system".

Group #3: Claim 30

Appellant's brief (pp. 14-15) argues that "downloading a virus scanning software utility program as well as a virus signature file, as in Reinert, fails to specifically suggest a technique "wherein said one or more malware detection files are determined based on a malware detection product" (emphasis added)." However, the similarly to the response applied to claim 29 above, it is submitted that since Reinert's malware detection product (Reinert's virus scanning program with communications program, Reinert col. 7, lines 62-67)

retrieves the malware detection files (up-to-date virus signature file, col. 8, lines 20-25), the downloaded malware detection files are determined based on the virus scanning program and the communications program (Reinert's malware detection product). In the realm of Reinert's invention, the malware detection files would not be downloaded without the malware detection product and thus are determined "based on the malware detection product".

Issue #2

Group #1: Claim 26

Appellant's brief (p. 15) argues that "such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1". Therefore, the Examiner submits that the rejections are reasonable for the reasons given above regarding Issue #1, Group #1.

Group #2: Claim 27

Appellant's brief (p. 15) argues that "such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1". Therefore, the Examiner submits that the rejections are reasonable for the reasons given above regarding Issue #1, Group #1.

Issue #3

Group #1: Claim 31

Appellant's brief (p. 16) argues that "such claims are not met by the prior art for the reasons argued with respect to Issue #1, Group #1". Therefore, the

Examiner submits that the rejections are reasonable for the reasons given above regarding Issue #1, Group #1.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

Michael Simitoski
/M. J. S./
Examiner, Art Unit 2134

/Gilberto Barron Jr/
Supervisory Patent Examiner, Art Unit 2132

Conferees:

/Kambiz Zand/
Supervisory Patent Examiner, Art Unit 2134

/G. B./
Supervisory Patent Examiner, Art Unit 2132